

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 2 月 2 7 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 5 0 2 4 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 5 0 2 4 3]

出 願 人 株式会社ルネサステクノロジ
Applicant(s):

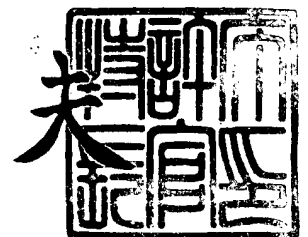
CERTIFIED COPY OF
PRIORITY DOCUMENT

BEST AVAILABLE COPY

2 0 0 4 年 2 月 1 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 K03003931A

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/00

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 水島 永雅

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 角田 元泰

【発明者】

 【住所又は居所】 東京都小平市上水本町五丁目 2 0 番 1 号 株式会社日立製作所半導体グループ内

 【氏名】 片山 国弘

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【先の出願に基づく優先権主張】

 【出願番号】 特願2003- 28998

 【出願日】 平成15年 2月 6日

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9902691

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 メモリカード

【特許請求の範囲】

【請求項 1】

外部のホスト機器と接続するためのインターフェイスと、
前記アプリケーションプログラムを格納可能で、前記アプリケーションプログラムを実行可能な IC カードチップと、
前記アプリケーションプログラムに関係した関係データを格納可能な不揮発性メモリと、
前記インターフェイスと前記 IC カードチップと前記不揮発性メモリに接続されたコントローラとを備え、
前記コントローラは、前記ホスト機器から前記インターフェイスで受信された特定コマンドに応答して、前記 IC カードチップと前記不揮発性メモリの間の前記関係データの転送を実行して、前記インターフェイスを介した前記ホスト機器への前記関係データの転送を禁止するメモリカード。

【請求項 2】

請求項 1 に記載のメモリカードにおいて、
前記 IC カードチップは、前記複数のアプリケーションプログラムを格納及び実行可能で、
前記不揮発性メモリは、複数のブロックに分割され、
前記複数のブロックの各ブロックは、各アプリケーションプログラムに割り当てられ、各関係データを格納可能であるメモリカード。

【請求項 3】

請求項 2 に記載のメモリカードにおいて、
前記不揮発性メモリは、前記アプリケーションプログラムを識別するためのアプリケーション ID と、前記不揮発性メモリから前記 IC カードチップへの前記関係データの転送のためのオペレーションコードを対応づけて格納する管理領域を有するメモリカード。

【請求項 4】

請求項 3 に記載のメモリカードにおいて、

前記 IC カードチップに少なくとも 1 つのアプリケーションプログラムを格納した場合に、前記 IC カードチップに格納されたアプリケーションプログラムに対応する前記不揮発性メモリ内の前記アプリケーション ID の変更又は追加又は削除を禁止するロック機能と前記ロック機能を解除するアンロック機能を有するメモリカード。

【請求項 5】

請求項 3 又は 4 に記載のメモリカードにおいて、

前記コントローラは、前記 IC カードからのアプリケーション ID と前記不揮発性メモリからのアプリケーション ID とを比較し、両者が一致した場合に、前記 IC カードチップと前記不揮発性メモリの間の前記関係データの転送を許可するメモリカード。

【請求項 6】

請求項 1 ～ 5 の何れかに記載のメモリカードにおいて、

前記関係データは、最初の使用から前記不揮発性メモリに格納されるメモリカード。

【請求項 7】

請求項 6 に記載のメモリカードにおいて、

前記関係データは、前記 IC カードチップ内のメモリに格納されることなく、最初の使用から前記不揮発性メモリに格納されるメモリカード。

【請求項 8】

請求項 1 ～ 7 の何れかに記載のメモリカードにおいて、

前記特定コマンドに応答した前記関係データの転送の実行及び禁止は、前記不揮発性メモリから前記 IC カードチップへの前記アプリケーションプログラムに対応する制御コマンドによって制御されるメモリカード。

【請求項 9】

複数のブロックに分割されたメモリと、IC カードチップと、前記メモリ及び前記 IC カードチップへのアクセスを制御するコントローラを備えたメモリカードにおいて、

前記メモリの各ブロックは、前記 I C カードチップによって実行されるアプリケーションプログラムのために前記アプリケーションプログラムごとに割り当てられ、

前記メモリは、前記 I C カードチップから前記コントローラへ指示する処理の内容を前記コントローラから前記 I C カードチップへ問い合わせるためのコマンドを記憶可能で、

前記 I C カードチップは、当該 I C カードチップが実行すべきアプリケーションプログラムのアプリケーション I D を前記コントローラへ送出し、

前記コントローラは、前記メモリ内の特定コマンドのうち前記 I C カードチップからの前記アプリケーションプログラム I D に対応する前記コマンドを特定し、特定された前記コマンドを前記 I C カードチップへ送出し、

前記 I C カードチップは、前記コントローラからの前記コマンドに応答して、前記処理の内容を前記コントローラへ指示し、

前記コントローラは、前記 I C カードチップからの指示に応答して、前記処理を実行するメモリカード。

【請求項 1 0】

請求項 9 に記載のメモリカードにおいて、

前記コマンドは、前記メモリのブロックへ書き込むべきデータを前記 I C カードチップから前記コントローラへ転送するための第 1 の転送コマンドと、前記メモリのブロックから読み出されたデータを前記コントローラから前記 I C カードチップへ転送するための第 2 の転送コマンドとを含むメモリカード。

【請求項 1 1】

請求項 1 0 に記載のメモリカードにおいて、

前記コマンドは、外部のホスト機器からのコマンドと異なるメモリカード。

【請求項 1 2】

複数のブロックに分割されたメモリと、 I C カードチップと、前記メモリ及び前記 I C カードチップへのアクセスを制御するコントローラを備えたメモリカードにおいて、

前記コントローラは、外部のホスト機器からの第 1 のコマンドに応答して、前

記メモリのブロックの利用権を、前記 I C カードチップによって実行されるべきアプリケーションプログラムのために前記アプリケーションプログラムごとに割り当て、

前記コントローラは、前記ホスト機器からの第 2 のコマンドに応答して、前記第 1 のコマンドに応答した処理を実行可能なアンロック状態から前記第 1 のコマンドに応答した処理を拒否するロック状態へ遷移するメモリカード。

【請求項 1 3】

請求項 1 2 に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプリケーションプログラムの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記アンロック状態である場合に、前記管理情報の内容の変更を許可し、

前記コントローラは、前記ロック状態である場合に、前記管理情報の内容の変更を禁止するメモリカード。

【請求項 1 4】

請求項 1 2 に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプリケーションプログラムの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記ブロックの利用権を前記アプリケーションプログラムのために割り当てる場合に、前記ブロックの識別子に対応する前記アプリケーションプログラムの識別子を前記管理情報に追加するメモリカード。

【請求項 1 5】

請求項 1 2 に記載のメモリカードにおいて、

前記メモリは、前記第 1 のコマンドに応答した処理を実行可能か否かを識別するためのフラグを記憶可能で、

前記コントローラは、前記アンロック状態から前記ロック状態へ遷移する場合に、前記フラグの値を変更するメモリカード。

【請求項 1 6】

請求項 1 2 に記載のメモリカードにおいて、

前記コントローラは、前記ホスト機器からの第 3 のコマンドに応答して、前記ロック状態から前記アンロック状態へ遷移するメモリカード。

【請求項 1 7】

請求項 1 6 に記載のメモリカードにおいて、

前記メモリは、前記第 3 のコマンドに応答した処理を許可するための参照パスワードを記憶可能で、

前記コントローラは、前記ホスト機器から受け取ったパスワードと前記メモリ内の前記参照パスワードとが一致した場合に、前記第 3 のコマンドに応答して、前記ロック状態から前記アンロック状態へ遷移するメモリカード。

【請求項 1 8】

請求項 1 2 に記載のメモリカードにおいて、

前記コントローラは、前記ホスト機器からの第 4 のコマンドに応答して、前記アプリケーションプログラムのために割り当てられた前記ブロックの利用権を解除するメモリカード。

【請求項 1 9】

請求項 1 8 に記載のメモリカードにおいて、

前記メモリは、前記ブロックの識別子と前記ブロックの利用権が割り当てられたアプリケーションプログラムの識別子との対応を管理するための管理情報を記憶可能で、

前記コントローラは、前記アプリケーションプログラムのために割り当てられた前記ブロックの利用権を解除する場合に、前記ブロックの識別子に対応する前記アプリケーションプログラムの識別子を前記管理情報から削除するメモリカード。

【請求項 2 0】

請求項 1 2 に記載のメモリカードにおいて、

前記メモリは、前記ホスト機器から受け取ったデータを記憶するための第 1 のエリアと、前記アプリケーションプログラムのために前記ブロックの利用権が割

り当てられた第 2 のエリアとを有するメモリカード。

【請求項 2 1】

請求項 2 0 に記載のメモリカードにおいて、

前記コントローラは、前記メモリの前記第 2 のエリアへ書き込むべきデータを前記 I C カードチップから受信し又は前記第 2 のエリアから読み出されたデータを前記 I C カードチップへ送信するための転送コマンドを前記アプリケーションプログラムごとに生成するメモリカード。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、セキュリティ機能を搭載した記憶装置及びその記憶装置が挿入可能なホスト機器及びその記憶装置を備えたホスト機器に係り、フラッシュメモリチップとコントローラチップと I C カードチップを有するメモリカード等に関する。

【0 0 0 2】

【従来の技術】

特許文献 1 には、I C モジュールと大容量のフラッシュメモリを搭載するメモリカードが記載されている。

【0 0 0 3】

特許文献 2 には、アプリケーションプログラムごとの実行必須条件を I C カードに記憶させておき、処理要求があった時に実行必須条件を充足していれば実行可能とし、充足していなければ実効不能とすることが記載されている。

【0 0 0 4】

特許文献 3 には、I C カード内のメモリ領域のうち、銀行のために領域 A が、病院のために領域 B が、それぞれ割り付けられていることが記載されている。

【0 0 0 5】

【特許文献 1】 特開平 10-198776 号公報

【特許文献 2】 特開 2000-66882 号公報

【特許文献 3】 特開平 6-222980 号公報

【0006】**【発明が解決しようとする課題】**

しかし、何れの従来技術も、ICカードのアプリケーションプログラム（アプレット）ごとに、分割された記憶エリアを割り当てることまでは記載されていない。よって、従来技術では、各アプリケーションプログラムが互いのメモリ内のデータを不正に侵害することが懸念される。

【0007】

本発明の目的は、特定のアプリケーションプログラムに係る処理を実行する場合に、特定のアプリケーションプログラムに係るデータをメモリ装置内部で処理することにより、特定のアプリケーションプログラムに係る処理の安全性を向上するメモリ装置を提供することである。

【0008】

本発明の目的は、ICカードチップのアプリケーションプログラム間のデータ干渉、即ち、あるアプリケーションプログラムに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制できる記憶媒体を提供することである。

【0009】**【課題を解決するための手段】**

本発明は、コントローラが、ホスト機器からインターフェイスで（例えば、外部端子）受信された特定コマンドに応答して、ICカードチップと不揮発性メモリ（例えば、フラッシュメモリの間のアプリケーションプログラムに関係した関係データ（例えば、アプリケーションプログラムによって処理されるべきデータ）の転送を実行して、インターフェイスを介したホスト機器への関係データの転送を禁止する。

【0010】

また、本発明は、メモリを複数のブロックに分割し、ブロックの使用権をICカードチップのアプリケーションプログラムごとに割り当てた。つまり、メモリが、ホスト機器からのデータを記憶するための第1の記憶エリア（例えば、ノーマルデータエリア）とICカードチップからのデータを記憶するための第2の記

憶エリア（例えば、セキュアデータエリア）を有し、さらに、第2の記憶エリアが複数のブロックに分割され、さらに各ブロックがアプリケーションプログラムごとに割り当てられる。

【0011】

また、本発明は、ホスト機器からコマンドによって、ブロックの使用権の割り当て、割り当て解除、割り当て及び解除の禁止、割り当て及び解除の禁止の解除を行うようにした。つまり、本発明は、ホスト機器からの第1のコマンド（例えば、アプレット登録コマンド）に応答してメモリのブロックの利用権をアプリケーションプログラムごとに割り当て、ホスト機器からの第2のコマンド（例えば、管理テーブルロックコマンド）に応答してアンロック状態からロック状態へ遷移する。さらに、ホスト機器からの第3のコマンド（例えば、管理テーブルアンロックコマンド）に応答してロック状態からアンロック状態へ遷移し、ホスト機器からの第4のコマンド（例えば、アプレット登録解除コマンド）に応答してアプリケーションプログラムのために割り当てられたブロックの利用権を解除する。

【0012】

【発明の実施の形態】

以下、本発明の一実施形態について説明する。

【0013】

図1は、本発明を適用したMultiMediaCard (MultiMediaCardはInfineon Technologies AGの登録商標である。以下、「MMC」と略記する。)の内部構成図を簡単に表したものである。MMC110は、MultiMediaCard仕様に準拠するのが好ましい。MMC110は、外部に接続したホスト機器160がMultiMediaCardのプロトコル仕様に準拠したメモリカードコマンドを発行することによって、ファイルデータを読み書きすることができるストレージ機能や、機密データ保護や個人認証などに必要な暗号演算をおこなうことができるセキュリティ処理機能を有する。ホスト機器160は、例えば、携帯電話、携帯情報端末(PDA)、パーソナルコンピュータ、音楽再生(及び録音)装置、カメラ、ビデオカメラ

、自動預金預払器、街角端末、決済端末等が該当する。MMC 110は、MMC外部端子140、コントローラチップ120、フラッシュメモリチップ130、ICカードチップ150を持つ。フラッシュメモリチップ130は、不揮発性の半導体メモリを記憶媒体とする大容量（例えば、64メガバイト）のメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。MMC外部端子140は7つの端子から構成され、外部のホスト機器160と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。コントローラチップ120は、MMC 110内部の他の構成要素（MMC外部端子140、フラッシュメモリチップ130、ICカードチップ150）と接続されており、これらを制御するマイコンチップである。ICカードチップ150は、ICカードのプラスチック基板中に埋め込むためのマイコンチップであり、その外部端子、電気信号プロトコル、コマンドはISO/IEC 7816規格に準拠している。ICカードチップ150の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子、グランド端子がある。ICカードチップ150の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子がコントローラチップ120に接続されている。コントローラチップ120は、ICカードチップ150の外部端子からICカードチップ150にICカードコマンドを発行することによって、外部のホスト機器160から要求されたセキュリティ処理に必要な演算をおこなう。ICカードチップ150は、演算処理を行うためのCPU 151と、EEPROM（Electrically Erasable Programmable Read Only Memory）152とを備える。一方、フラッシュメモリチップ130には、記憶素子を備えるが、マイコンは存在しない。

【0014】

セキュリティ処理は、例えば、ICカードチップ150内のEEPROM 152にデータが書き込まれるとき、又は、EEPROM 152からデータが読み出されるときにCPU 151により実行される。セキュリティ処理の詳細な内容は、EEPROM 152内に格納されたプログラムコードによって記述されている

。多種多様なセキュリティ処理に適用できるように、そのプログラムコードは機能的に異なる複数のモジュールとして構成されている。CPU151は必要に応じてセキュリティ処理に使用するモジュールを切り替えることができる。以下、このモジュール単位をアプレットと呼ぶ。例えば、EEPROM152は、アプレットA153とアプレットB154とを格納する。ICカード内の各アプレットはそれぞれ、自身のアプリケーション識別子（以下、AID（Application Identifier）と呼ぶ。）を所有する。図1において、アプレットA153のAIDは155として、アプレットB154のAIDは156として示されている。これらのAIDは、ICカードのアプリケーションプログラムを識別するために、国際的にユニークに割り振られた値であることが好ましい。国際的に流通するAIDの付番方法は、国際規格としてISO/IEC7816-5で規定されている。EEPROM152の記憶容量は例えば64キロバイトであり、フラッシュメモリチップ130の記憶容量より小さい。但し、本発明を実施する上で、EEPROM152の記憶容量は、フラッシュメモリチップ130の記憶容量と同じでもよいし、大きくてもよい。

【0015】

ICカードチップ150には、セキュリティ評価基準の国際標準であるISO/IEC15408の評価・認証機関によって認証済みである製品を利用する。一般に、セキュリティ処理をおこなう機能を持つICカードを実際の電子決済サービスなどで利用する場合、そのICカードはISO/IEC15408の評価・認証機関による評価と認定を受ける必要がある。MMCにセキュリティ処理をおこなう機能を追加することによってMMC110を実現し、それを実際の電子決済サービスなどで利用する場合、MMC110も同様にISO/IEC15408の評価・認証機関による評価と認定を受ける必要がある。MMC110は、評価・認証機関によって認証済みのICカードチップ150を内蔵し、そのICカードチップ150を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、MMC110はISO/IEC15408に基づくセキュリティ評価基準を容易に満足することができ、MMCにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【0016】

MMC110は、MultiMediaCard仕様に準拠した外部インタフェースを持つのが好ましい。MMC110は、一種類の外部インタフェースを通じて、MultiMediaCard仕様に準拠した標準メモリカードコマンドに加えて、セキュリティ処理を実行するコマンド（以下、セキュアライトコマンドと呼ぶ。）を受け付ける。セキュアライトコマンドは入力データを伴う。コントローラチップ120は、MMC110が受信したコマンドが標準メモリカードコマンドであるか、セキュアライトコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。標準メモリカードコマンドを受信したならば、フラッシュメモリチップ130を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュアライトコマンドを受信したならば、ICカードチップ150を選択し、これにICカードコマンドを発行してセキュリティ処理を実行することができる。ここで発行されるICカードコマンドは、セキュアライトコマンドによって入力されるデータ（以下、セキュアライトデータと呼ぶ。）の中に埋め込まれている。ICカードチップ150はこのコマンドに応じてICカードレスポンスを返すが、コントローラチップ120はそれをキャッシュする。さらに、MMC110は、一種類の外部インタフェースを通じて、セキュリティ処理の結果を読み出すコマンド（以下、セキュアリードコマンドと呼ぶ。）も受け付ける。セキュアリードコマンドは出力データを伴う。セキュアリードコマンドを受信したならば、キャッシュしておいたICカードレスポンスを含むデータ（以下、セキュアリードデータと呼ぶ。）を出力する。

【0017】

図2は、本発明を適用したMMC110の動作を概念的に示すフローチャートである。以下、図2を参照しながらその動作を説明する。ホスト機器160はMMC110にセキュアライトコマンドを送信すると（201）、コントローラチップ120はICカードチップ150にICカードコマンドを送信する（202）。ICカードチップ150はICカードコマンドを受信すると（203）、そのとき選択されているアプレットのAIDを含むICカードレスポンスをコント

ローラチップ120に返信する(204)。コントローラチップ120がそのICカードレスポンスを受信したらフラッシュメモリチップ130にリードコマンドを送信する(205)。これにより、フラッシュメモリチップ130はAIDのリスト(事前書き込んで置くものとする。)を読み出して(206)、コントローラチップ120に出力する。コントローラチップ120はそのリストから、ICカードチップ150からのAIDに一致するものがあるか検索する(207)。一致するAIDを検出できないならば、ホスト機器160からセキュアリードコマンドを受けてICカードレスポンスをセキュアリードデータとして送信し(219)、ホスト機器160がそれを受信する(220)。一方、ステップ207で、AIDを検出したならば、ICカードレスポンスをホスト機器160に出力するのを禁止し、ICカードチップ150にICカードコマンドを送信する(208)。ICカードチップ150がこのICカードコマンドを受信すると(209)、選択されているアプレットは、ICカードチップ150とフラッシュメモリチップ130との間でデータを転送するため、データ転送方向に応じたICカードレスポンスを作成する。ICカードからフラッシュへ転送したいならば、フラッシュメモリにライトするデータとそのアドレスを含んだICカードレスポンスを作成して返信する(211)。フラッシュからICカードへ転送したいならば、フラッシュメモリからリードしたいアドレスを含んだICカードレスポンスを作成して返信する(214)。ステップ211のあと、コントローラチップ120はフラッシュメモリチップ130にライトコマンドを送信する(212)。これに対し、フラッシュメモリチップ130は指定されたアドレスにデータを書き込む(213)。これにより、ICカードからフラッシュへのデータ転送が完了する。一方、ステップ214のあと、コントローラチップ120はフラッシュメモリチップ130にリードコマンドを送信する(215)。これに対し、フラッシュメモリチップ130は指定されたアドレスからデータを読み出し(216)、コントローラチップ120に出力する。コントローラチップ120は、そのリードデータをICカードコマンドによってICカードチップ150に送信し(217)、ICカードチップ150がこれを受信する(218)。これにより、フラッシュからICカードへのデータ転送が完了する。 図6は、セキュア

ライトデータおよびセキュアリードデータのフォーマットの一例を示したものである。このフォーマットは、実行するセキュリティ処理の内容が1つのICカードコマンドで表現でき、セキュリティ処理の結果が1つのICカードレスポンスで表現できる場合に適用することが好ましい。上述の通り、ICカードチップ150に送信するICカードコマンド、ICカードチップ150から受信するICカードレスポンスはともにISO/IEC 7816-4規格に従う。本規格によれば、ICカードコマンドの構成は、4バイトのヘッダ（クラスバイトCLA、命令バイトINS、パラメータバイトP1とP2）が必須であり、必要に応じて、入力データ長指示バイトLc、入力データフィールドDataIn、出力データ長指示バイトLeが後に続く。また、ICカードレスポンスの構成は、2バイトのステータスSW1とSW2が必須であり、必要に応じて、出力データフィールドDataOutがその前に置かれる。本フォーマットにおけるセキュアライトデータ601は、ICカードコマンド602の前にICカードコマンド長Lca604を付け、さらにICカードコマンド602の後にダミーデータ605をパディングしたものである。Lca604の値はICカードコマンド602の各構成要素の長さを合計した値である。一方、セキュアリードデータ611は、ICカードレスポンス612の前にICカードレスポンス長Lra614を付け、さらにICカードレスポンス612の後にダミーデータ615をパディングしたものである。Lra614の値はICカードレスポンス612の各構成要素の長さを合計した値である。なお、この図では、ICカードコマンドにLc、DataIn、Leが含まれ、ICカードレスポンスにDataOutが含まれる場合のフォーマット例を表している。MMC 110に対する標準メモリカードコマンドに含まれるデータリード/ライトコマンドの仕様では、リード/ライトアクセスするデータを固定長のブロック単位で処理することが基本となっている。よって、セキュアライトデータ601やセキュアリードデータ611のサイズも、MMC 110の標準メモリカードコマンドの仕様に準拠したブロックサイズに一致させることが好ましい。ダミーデータ605、615は、セキュアライトデータ601やセキュアリードデータ611のサイズをブロックサイズに一致させるために適用される。ブロックサイズとして採用する値は、一般の小型メモリカード

が論理ファイルシステムに採用している F A T 方式におけるセクタサイズ（5 1 2 バイト）が望ましい。パディングするダミーデータ 6 0 5、6 1 5 は全てゼロでもよいし、乱数でもよいし、コントローラチップ 1 2 0 やホスト機器 1 6 0 がデータエラーを検出したり訂正するためのチェックサムでもよい。L c a 6 0 4 の値はコントローラチップ 1 2 0 がセキュアライトデータ 6 0 1 からダミーデータ 6 0 5 を除去して I C カードコマンド 6 0 2 を抽出するために使用し、L r a 6 1 4 の値はホスト機器 1 6 0 がセキュアリードデータ 6 1 1 からダミーデータ 6 1 5 を除去して I C カードレスポンス 6 1 2 を抽出するために使用する。

【0 0 1 8】

コントローラチップ 1 2 0 は、電源供給端子、クロック入力端子を通して、I C カードチップ 1 5 0 への電源供給、クロック供給を制御する。ホスト機器 1 6 0 からセキュリティ処理を要求されないときには、I C カードチップ 1 5 0 への電源供給やクロック供給を停止させることができ、MMC 1 1 0 の電力消費を削減することができる。

【0 0 1 9】

電源供給されていない I C カードチップ 1 5 0 を、I C カードコマンドを受信できる状態にするには、まず、I C カードチップ 1 5 0 に電源供給を開始し、リセット処理を施すことが必要である。コントローラチップ 1 2 0 は、MMC 1 1 0 がホスト機器 1 6 0 からセキュアライトコマンドを受信したのを契機に、電源供給端子を通して I C カードチップ 1 5 0 への電源供給を開始する機能を持つ。また、コントローラチップ 1 2 0 は、MMC 1 1 0 がホスト機器 1 6 0 からセキュアライトコマンドを受信したのを契機に、リセット入力端子を通して I C カードチップ 1 5 0 のリセット処理をおこなう機能を持つ。コントローラチップ 1 2 0 は、セキュアライトコマンドを受信するまで I C カードチップ 1 5 0 への電源供給を停止させておくことができる。したがって、MMC 1 1 0 の電力消費を削減することができる。

【0 0 2 0】

コントローラチップ 1 2 0 は、I C カードチップ 1 5 0 のクロック入力端子を通して I C カードチップ 1 5 0 に供給するクロック信号を MMC 1 1 0 内部で発

生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を持つ。MMC外部端子140のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器160によるタイミング解析、電力差分析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【0021】

フラッシュメモリチップ130は、ノーマルデータエリア131と管理エリア132とセキュアデータエリア133とを含む。

【0022】

ノーマルデータエリア131は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器160が標準メモリカードコマンドを使用することにより指定した論理アドレスにデータを読み書きできる領域である。

【0023】

セキュアデータエリア133は、ICカードチップ150内のEEPROM152に格納されたアプレット（例えば、153や154）をCPU151が実行する際に（すなわち、セキュリティ処理を実行する際に）、扱うデータを格納することができる領域である。セキュアデータエリア133は複数のブロックに分割されている。これをセキュアデータブロックと呼ぶ。例えば、セキュアデータエリア133は4つのセキュアデータブロック133a、133b、133c、133dで構成される。セキュアデータブロックは、コントローラチップ120がアプレットごとにその利用権を割り当てることができる単位である。例えば、アプレットA153はセキュアデータブロックc133cの利用権を持ち、アプレットB154はセキュアデータブロックa133aの利用権を持つ。また、各セキュアデータブロックは複数の固定長データレコードに分割されている。例えば、1レコードのサイズは128バイトであり、1つのセキュアデータブロック当たり8192個のレコードで構成される。このとき、1つのセキュアデータブロックのサイズが1メガバイトとなり、セキュアデータエリア133の容量は4メガバイトとなる。したがって、EEPROM152に格納されたアプレットは、セキュアデータエリア133に格納されたデータにアクセスすることによって、EEPROM152の容量以上の不揮発データを利用できる。例えば、ICカ

ードチップ 1 5 0 内のアプレット A 1 5 3 が電子決済に関するセキュリティ処理のためのプログラムである場合、決済ログ（支払金額や日時など）をセキュアデータエリア 1 3 3 に格納することにより、EEPROM 1 5 2 のみを利用するよりも多くの決済ログが保存でき、ユーザの利便性が高くなる。IC カードチップ 1 5 0 からセキュアデータエリア 1 3 3 へのアクセス（ライトやリード）は、IC カードチップ 1 5 0 からの要求に基づいてコントローラチップ 1 2 0 が実行するが、その要求の発生条件は IC カードアプレットの任意である。例えば、EEPROM 1 5 2 の容量が何らかのしきい値以下になった（ゆえにカード外部に記録せざるを得ない）こと、IC カードチップ内のデータが何らかの保護基準に満たない（ゆえにカード外部に記録しても問題ない）こと、EEPROM 1 5 2 の中に所望のデータが見つからない（ゆえにカード外部から読み込む）こと、などが挙げられる。IC カードチップ 1 5 0 からセキュアデータエリア 1 3 3 へのアクセスの詳細な手順については後に述べる。

【0 0 2 4】

一方、管理エリア 1 3 2 は、コントローラチップ 1 2 0 がセキュアデータエリア 1 3 3 を管理するための情報を格納する領域である。コントローラチップ 1 2 0 は、MMC 1 1 0 がホスト機器 1 6 0 からセキュアライトコマンドを受信したことを契機に、この領域に情報を格納したり、削除したりする。そのコマンドについては後述する。管理エリア 1 3 2 は、ロックフラグ 1 3 4 とパスワードエリア 1 3 5 と管理テーブル 1 3 6 とを含む。

【0 0 2 5】

管理テーブル 1 3 6 は、セキュアデータエリア 1 3 3 を構成している各セキュアデータブロックの利用権を持つアプレットを登録するための領域である。アプレットを識別するために、この領域に A I D を格納することによってアプレットを登録することが望ましい。A I D を利用することにより、セキュアデータエリア 1 3 3 を使用するアプレットを確実に識別することができる。コントローラチップ 1 2 0 は、A I D 1 3 7 に同一の A I D を複数格納することを禁止する。管理テーブル 1 3 6 のブロックの欄は、セキュアデータブロックを識別するためのブロック識別子としてブロックの先頭アドレス値を登録する。但し、先頭アドレ

ス値の代わりにMMC内でユニークな番号をブロック識別子として登録してもよい。尚、管理テーブル136の代わりに、各セキュアデータブロック内に直接にAIDを登録)してもよい。

【0026】

管理テーブル136には、AID137だけでなく、アプレットごとに転送コマンドコード138を格納することができる。この転送コマンドコード138は、コントローラチップ120がセキュアデータブロックの利用権を、アプレットのために割り当てる時に、コントローラチップ120によって生成されるのは好ましい。転送コマンドコードとは、“ライト転送コマンド”および“リード転送コマンド”それぞれのコマンドAPDU (Application Protocol Data Unit) のCLAバイトとINSバイトに設定する2バイト×2個の値である。ここで、“ライト転送コマンド”および“リード転送コマンド”とは、セキュアデータエリア133にレコードデータをライトする前、あるいはそこからレコードデータをリードした後に、コントローラチップ120とICカードチップ150との間でそのレコードデータを転送するために、コントローラチップ120がICカードチップ150に対して発行するICカードコマンド形式のコマンドである。特に、コントローラチップ120へレコードデータを送り出すためのコマンドをライト転送コマンドと呼び、ICカードチップ150へレコードデータを送り込むためのコマンドをリード転送コマンドと呼ぶ。これらのコマンドの詳細な説明は後述する。セキュアデータエリア133の利用権を持つアプレット(153や154)には、ライト／リード転送コマンドを受信した際にレコードデータを扱う処理プログラムが記述されている。転送コマンドコード138はアプレットごとに個別に決められるようになっている。もし、転送コマンドコードが全てのアプレットに共通の固定値であるならば、ホスト機器160からのセキュアライトデータに含まれるアプレット特有のコマンドとライト／リード転送コマンドとの間でコーディングの競合が発生する可能性がある。本発明によれば、このようなコーディング競合を防ぐことができる。なお、転送コマンドコード138のうちINSコードに関しては、伝送プロトコルの都合上ISO/IEC7816-3に準拠していなければならない。

【0027】

ロックフラグ134は、管理テーブル136に格納された登録情報の変更の可否を示す1バイトのデータを格納する領域である。この領域にFFhを設定することで管理テーブル136の情報の変更が禁止状態（ロック状態）であることを示す。また、00hを設定することで管理テーブル136の情報の変更が許可状態（アンロック状態）であることを示す。

【0028】

パスワードエリア135は、管理テーブル136の情報をアンロック状態にするための255バイトのパスワードの参照値を格納しておく領域である。管理テーブル136の情報をロックする時には必ず、ホスト機器160からセキュアライトコマンドにより、255バイトのパスワード参照をこの領域に設定する。管理テーブル136の情報をアンロック状態にする場合は、ホスト機器160からセキュアライトコマンドにより、ロック時に設定したパスワード参照と同じパスワードを入力する必要がある。入力したパスワードとパスワード参照との一致によって、管理テーブル136の情報の変更をアンロックすることができる。

【0029】

管理エリア132は、ホスト機器160が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ120により物理的にアクセス制限がかけられている。つまり、管理エリア132はコントローラチップ120による論理アドレスが割り振られていないため、ホスト機器160が直接データを読み書きできない。したがって、MMC110のセキュリティ処理の信頼性や安全性が向上する。

【0030】

以下、図3を参照しながら、セキュアデータエリア133に対するレコードデータのライト／リードアクセスにおいて用いられるライト／リード転送コマンドのコマンドAPDUとレスポンスAPDUについて詳細に述べる。

【0031】

図2aは、ICカードチップ150が出力するレスポンスAPDUを示している。このレスポンスAPDU300に含まれるDataOut304の先頭2バ

イト（以下、先頭から順に第1制御バイト301、第2制御バイト302と呼ぶ。）、およびSW1バイト305とSW2バイト306に特別な値を設定することにより、ICカードチップ150はコントローラチップ120にセキュアデータエリア133に対するアクセス要求を通知することができる。なお、後続出力データ303（Data Out 304のうち第1制御バイト301と第2制御バイト302を除いた部分）は、アクセス要求に必要な情報を送信するために使用される。

【0032】

ICカードチップ150は、コントローラチップ120に対してセキュアデータエリア133へアクセスすることを要求するため、SW1バイト305とSW2バイト306に90FFhという専用のステータス値を設定しなければならない。コントローラチップ120は、ICカードチップ150が出力するレスポンスAPDUを常に監視し、SW1バイト305とSW2バイト306の値が90FFhであることを検出したら、その前方にあるData Out 304の第1制御バイト301、第2制御バイト302第1制御バイト第2制御バイトを調査し、要求されたアクセスの内容などを認知する。一方、90FFhでなかった場合は、このレスポンスAPDUを含むセキュアリードデータをホスト機器160に出力する。ただし、SW1バイト305とSW2バイト306の値が90FFhであっても、条件によって、そのままホスト機器160に出力されることがある。その詳細は後述する。

【0033】

コントローラチップ120は、セキュアデータエリア133へのアクセスを開始するとき、ICカードチップ150上で選択されているアプレットが何であるかによって、133a～133dの中からアクティブにするセキュアデータブロックを選択する。アクセスすべきセキュアデータブロックの選択は、ICカードチップ150からアクセス開始要求が発生した直後におこなう。アクセス開始要求のためにData Out 304に設定するデータの仕様を以下に示す。第1制御バイト301の上位4ビットには、0001を設定する。第1制御バイト301の下位4ビットには、アクセスモードを示すコードを設定する。ここで指定可

能なアクセスモードには、レコードデータのライト、レコードデータのリードの2種類がある。0001というコードはレコードデータのライト、0010というコードはレコードデータのリードである。その他のコードは無効である。また、後続出力データ303には、ICカードチップ150上で選択されているアプレットのAIDを設定する。例えば、アプレットA153が選択されているならばAID155を、アプレットB154が選択されているならばAID156を設定する。第2制御バイト302には、そのAIDの長さを設定する。

【0034】

コントローラチップ120は、第1制御バイトの上位4ビットが0001ならば、後続出力データ303に含まれるAIDで管理テーブル136内の全てのAID137を検索し、アクティブにすべきセキュアデータブロックを決定する。一致するAIDが見つからなかった場合は、このレスポンスAPDUを含むセキュアリードデータをホスト機器160に出力する。AIDを検出し、それに対応するセキュアデータブロックが判明した後、コントローラチップ120は、第1制御バイトの下位4ビットが0001ならばライト、0010ならばリードのアクセスを開始すると認識する。第1制御バイトの下位4ビットがそれ以外の場合は、このレスポンスAPDUを含むセキュアリードデータをホスト機器160に出力する。

【0035】

コントローラチップ120がアクセスモード（ライトまたはリード）を認知した後、そのモードに応じてライト／リード転送コマンドを発行することによって、アクティブなセキュアデータブロック対してライトすべきレコードデータ、またはリードしたレコードデータをICカードチップ150とコントローラチップ120との間で転送することができる。図3bと図3cはライト／リード転送コマンドのコマンドAPDUを示したものである。図3bはコントローラチップ120からICカードチップ150への転送データがない場合、図3cは転送データがある場合を示している。前述のように、ライト／リード転送コマンドのコマンドAPDU310（または320）のCLAバイト314（または326）とINSコード315（または327）にはあらかじめアプレットごとに登録され

たものを設定する。そのため、管理テーブル 1 3 6 から 2 バイト×2 個の転送コマンドコード 1 3 8 を読み出す。

【0 0 3 6】

ライト／リード転送コマンドのコマンド A P D U 3 1 0（または 3 2 0）では、直前のアクセスの結果を I C カードチップ 1 5 0 に通知するため、P 1 バイト 3 1 6（または 3 2 8）と P 2 バイト 3 1 7（または 3 2 9）に特殊な値を設定する。0 0 0 0 h は直前のアクセスにエラーがないことを意味する。8 0 X X h は直前のアクセスにエラーが発生したことを意味する。なお、X X はエラー内容を示す 1 6 進コードである。エラーの場合、アクティブなセキュアデータブロックへのデータアクセスは実行されない。よって、セキュアデータブロックのレコードデータの内容も変化しない。

【0 0 3 7】

I C カードチップ 1 5 0 は、ライト／リード転送コマンドのレスポンス A P D U 3 0 0 における後続出力データ 3 0 3 を用いて、ライトしたいレコード番号とレコードデータ、またはリードしたいレコード番号をコントローラチップ 1 2 0 に送信する。ライトモードでは、指定レコード番号（4 バイト）とライトデータ（1 2 8 バイト）の連結データを設定し、リードモードでは、指定レコード番号（4 バイト）を設定する。このように、後続出力データ 3 0 3 の長さはアクセスモードによって変わるので、ライト／リード転送コマンドのコマンド A P D U の L e バイト 3 1 3（または 3 2 5）には、アクセスモードに応じた値を設定する必要がある。ライトモードでは、後続出力データ 3 0 3 の長さが 8 4 h となるので D a t a O u t 3 0 4 の長さは 8 6 h となる。よって、L e バイト 3 1 3（または 3 2 5）には 8 6 h を設定する。リードモードでは、後続出力データ 3 0 3 の長さが 0 4 h となるので D a t a O u t 3 0 4 の長さは 0 6 h となる。よって、L e バイト 3 1 3（または 3 2 5）には 0 6 h を設定する。

【0 0 3 8】

アクセス開始直後の（つまり、最初に発行される）ライト／リード転送コマンドのコマンド A P D U は、図 3 b の形式となる。そのとき、P 1 バイト 3 1 6 と P 2 バイト 3 1 7 には、0 0 0 0 h を設定する。L e バイト 3 1 3 には、ライト

モードの場合 86 h を、リードモードの場合 06 h を設定する。

【0039】

ライト／リード転送コマンドのレスポンス APDU は、図 3 a の形式をとる。IC カードチップ 150 上で選択されているアプレットは、レスポンス APDU 300 を利用してアクティブなセキュアデータブロックに対するアクセス（ライト／リード）をコントローラチップ 120 に要求することができる。以下、これをアクセス実行要求と呼ぶ。第 1 制御バイト 301 と第 2 制御バイト 302 に設定するデータの仕様を以下に示す。第 1 制御バイト 301 の上位 4 ビットには、0010 を設定する。第 1 制御バイト 301 の下位 4 ビットには、要求するアクセスを示すコードを設定する。0001 というコードはレコードデータのライト、0010 というコードはレコードデータのリードである。その他のコードは無効である。このコードが表すアクセスモードは、コントローラチップ 120 が認めるアクセスモードに一致していなければならない。また、その第 2 制御バイト 302 によって、次のアクセスモード（ライト／リード）の要求をおこなうことができる。コントローラチップ 120 はこれを参照して、自身が認めるアクセスモードをスイッチする。

【0040】

コントローラチップ 120 は、第 1 制御バイト 301 の上位 4 ビットが 0010 ならば、アクティブなセキュアデータブロックに対して、指定されたレコード番号のデータをライト／リードする。ライト／リード処理が正常終了した場合（アクセス結果 312（または 322）の値が 0000 h）、第 2 制御バイト 302 が 01 h ならば自身が認めるアクセスモードをライトモードにスイッチ、02 h ならばリードモードにスイッチする。ライト／リード処理に何らかのエラーがあった場合（アクセス結果 312（または 322）の値が 80XX h）、自身が認めるアクセスモードをスイッチせずにエラーが起きた時点のものを維持する。

【0041】

コントローラチップ 120 が 2 回目以降に発行するライト／リード転送コマンドのコマンド APDU は、直前のアクセスの結果やアクセスモードの状態遷移によって、図 3 b の形式になったり、図 3 c の形式になったりする。また Le 31

3（または325）の値も変わる。その詳細を以下に示す。

【0042】

直前のライトアクセスが正常で次回もライトモードのとき、図3bの形式であり、アクセス結果312の値が0000hで、Le313の値は86hである。

【0043】

直前のライトアクセスが正常で次回がリードモードのとき、図3bの形式であり、アクセス結果312の値が0000hで、Le313の値は06hである。

【0044】

直前のリードアクセスが正常で次回もリードモードのとき、図3cの形式であり、アクセス結果322の値が0000hで、Lc323の値は80hで、DataIn324にはリードしたレコードデータが設定され、Le325の値は06hである。

【0045】

直前のリードアクセスが正常で次回がライトモードのとき、図3cの形式であり、アクセス結果322の値が0000hで、Lc323の値は80hで、DataIn324にはリードしたレコードデータが設定され、Le325の値は86hである。

【0046】

直前のライトアクセスがエラーのとき、図3bの形式であり、アクセス結果312の値が80XXhで、Le313の値は86hである。

【0047】

直前のリードアクセスがエラーのとき、図3bの形式であり、アクセス結果312の値が80XXhで、Le313の値は06hである。

【0048】

アクセスエラー時にアクセス結果312（または322）に設定する80XXhにおいて、エラー内容を示すコードXXの例を以下に示す。

【0049】

XX=01は、指定されたレコード番号がアクセス可能な範囲外であるエラーを意味する。

【 0 0 5 0 】

XX = 0 2 は、フラッシュメモリチップ 1 3 0 が故障などにより利用できないエラーを意味する。

【 0 0 5 1 】

XX = 0 3 は、第 1 制御バイト 3 0 1 の下位 4 ビットが現在のアクセスモードに合致しないエラーを意味する。

【 0 0 5 2 】

XX = 0 4 は、第 2 制御バイト 3 0 2 で要求された次のアクセスモードが不正であるエラーを意味する。

【 0 0 5 3 】

図 4 を参照しながら、I C カードチップ 1 5 0 内のアプレットが、セキュアデータエリア 1 3 3 にアクセスを開始するときの処理の流れ、およびライト／リード転送コマンドによってそこに対するアクセスを実行するときの処理の流れを説明する。

【 0 0 5 4 】

ホスト機器 1 6 0 は MMC 1 1 0 にセキュアライトコマンドを発行し（4 0 1）、セキュアライトデータ 6 0 1 を入力する（4 0 2）。コントローラチップ 1 2 0 は、セキュアライトデータ 6 0 1 から I C カードコマンドのコマンド A P D U 6 0 2 を抽出し（4 0 3）、それを用いて I C カードチップ 1 5 0 に I C カードコマンドを発行する（4 0 4）。

【 0 0 5 5 】

I C カードチップ 1 5 0 は、その I C カードコマンドを受信し（4 0 5）、セキュアデータエリア 1 3 3 へのアクセスを要求する I C カードレスポンス 3 0 0 を作成し、それを返信する（4 0 6）。コントローラチップ 1 2 0 は、このレスポンスを受信し、その SW 1 バイト 3 0 5 と SW 2 バイト 3 0 6 が 9 0 F F h であるかを調べる（4 0 7）。9 0 F F h でないならばステップ 4 0 8 に移る。9 0 F F h であるならば、第 1 制御バイト 3 0 1 の上位 4 ビットが 0 0 0 1（アクセス開始要求）であるかを調べる（4 1 2）。0 0 0 1 でないならばステップ 4 2 0 に移る。0 0 0 1 であるならば、管理テーブル 1 3 6 がロックされているか

調べる(413)。アンロックされているならばステップ408に移る。ロックされているならば、後続出力データ303に含まれるAIDで管理テーブル136上のAID137を検索する(414)。一致するAIDを検出したならば(415)、コントローラチップ120はアクセス開始要求を承認し、ステップ416に移る。検出しなければアクセス開始要求を却下し、ステップ408に移る。ステップ416では、検出したAID137に対応するセキュアデータブロックを選択し、それをアクティブにする。さらに、対応する転送コマンドコード138を取得する(417)。そして、第1制御バイト301の下位4ビットを調べて、開始するアクセスモードを取得し(418)、そのアクセスモードに応じて図3bに示すようなライト／リード転送コマンドを作成する(419)。その後、ステップ404に戻り、ICカードチップ150にライト／リード転送コマンドを発行する。

【0056】

ステップ420では、第1制御バイト301の上位4ビットが0010(アクセス実行要求)であるかを調べる。0010でないならばステップ408に移る。0010であるならば、アクティブなセキュアデータブロックが存在するか、また第1制御バイト301の下位4ビットがコントローラチップ120の認知するアクセスモードに合致するかを調べる(421)。いずれかが偽ならばステップ408に移る。両者とも真ならば、アクセス実行を承認し、後続出力データ303に含まれるレコード番号を取得する(422)。そして、そのレコード番号の指示するデータに対してライト／リードを実行する(423)。このとき、ライトモードの場合は、後続出力データ303に含まれる128バイトのデータをライトする。次に、そのアクセスの結果を示すコードを312または322に設定する(424)。そして、第1制御バイト301の下位4ビットを調べて、次のアクセスモードを取得し(418)、そのアクセスモードに応じて図3bまたは図3cに示すようなライト／リード転送コマンドを作成する(419)。その後、ステップ404に戻り、ICカードチップ150にライト／リード転送コマンドを発行する。

【0057】

ステップ408では、ICカードチップ150が返信したレスポンスAPDU 602からセキュアリードデータ611を作成する。ステップ408に至ることによって、セキュアデータエリア133へのアクセスは終了する。この後、ホスト機器160はセキュアリードコマンドを発行し(409)、コントローラチップ120はセキュアリードデータ611を出力する(410)。そして、ホスト機器160はセキュアリードデータ611を受信する(411)。

【0058】

以上より、ホスト機器160から一組のセキュアライト／セキュアリードコマンドをMMC110に処理させる間に、ICカードチップ150内のアプレットは任意の回数、セキュアデータエリア133へアクセスすることができる。

【0059】

以下、管理エリア132に関するアクセスについて説明する。

【0060】

ホスト機器160が管理エリア132の情報にアクセスできるように、MMC110は、以下の4つの管理コマンドに応じることができる。すなわち、(1) アプレット登録コマンド、(2) アプレット登録解除コマンド、(3) 管理テーブルロックコマンド、(4) 管理テーブルアンロックコマンドの4つである。(1) は、管理テーブル136にセキュアデータエリア133を利用するアプレットを登録し、アプレットが利用するセキュアデータブロックを割り当てるコマンド、(2) は、管理テーブル136からアプレットの登録情報を削除し、セキュアデータブロックの割り当てを解除するコマンド、(3) は、管理テーブル136上の登録情報の変更を禁止するコマンド、(4) は、管理テーブル上136の登録情報の変更を許可するコマンドである。これらのコマンドは、一般のセキュリティ処理と同じくセキュアライトコマンドとセキュアリードコマンドのプロトコルによって実施され、コントローラチップ120によって処理される。また、その際に入出力されるセキュアライトデータとセキュアリードデータに含まれるAPDU(図6における602や612)を利用して各処理(登録、登録解除、ロック、アンロック)に必要な情報を交換する。

【0061】

アプレット登録コマンドとアプレット登録解除コマンドでは、Data In 606にAIDを設定する。このAIDによって登録したいアプレットを指定する。AIDとセキュアデータブロックとをどのように対応付けるかはコントローラチップ120が決定する。ホスト機器160はセキュアデータブロックを直接指定できない。

【0062】

管理テーブルロックコマンドでは、Data In 606に255バイトのパスワードを設定する。そのパスワードはパスワードエリア135に設定され、ロックフラグ134がFFh（ロック状態）になる。これにより、アプレット登録コマンドとアプレット登録解除コマンドが無効になる。すでにロック状態だった場合は、そのパスワードはパスワードエリア135に設定されず、アプレット登録コマンドとアプレット登録解除コマンドは有効のままとなる。

【0063】

管理テーブルアンロックコマンドでは、Data Inに255バイトのパスワードを設定する。そのパスワードはパスワードエリア135に設定された値と一致比較され、一致したならばロックフラグ134が00h（アンロック状態）になる。これにより、アプレット登録コマンドとアプレット登録解除コマンドが有効になる。すでにアンロック状態だった場合は、アプレット登録コマンドとアプレット登録解除コマンドは無効のままとなる。

【0064】

アプレット登録コマンドとアプレット登録解除コマンドが有効な状態（アンロック状態）では、パスワードを知らないホスト機器160によって管理テーブル136の情報が不正に変更され、あるアプレットが、それ自身がアクセス可能なセキュアデータブロック以外のセキュアデータブロックをライト／リードするという不正アクセスが発生しうる。そこで、コントローラチップ120は、ロックフラグ134の値が00h（アンロック状態）では、ICカードチップ150内で選択されているアプレットがセキュアデータエリアへアクセスするのを許可しない。ホスト機器160は、管理テーブル136の登録情報の設定／変更後は、管理テーブルロックコマンドにより必ずロックフラグ134をFFhに設定しな

ければならない。

【0065】

図5を参照しながら、上記4つの管理コマンドの処理の流れを説明する。

【0066】

ホスト機器160はMMC110にセキュアライトコマンドを発行し(501)、セキュアライトデータ601を入力する(502)。コントローラチップ120は、セキュアライトデータ601からICカードコマンドのコマンドAPDU602を抽出し(503)、それが管理コマンドであるかを調べる(504)。管理コマンドならばステップ507に移る。一方、管理コマンドでないならば、そのコマンドAPDU602を用いてICカードチップ150にICカードコマンドを発行し(505)、ICカードチップ150からそのレスポンスを受信し(506)、ステップ527に移る。

【0067】

ステップ507では、コントローラチップ120は、コマンドAPDU602がアプレット登録コマンドを示すものかを調べる。アプレット登録コマンドならばステップ511に移る。さもなくば、それがアプレット登録解除コマンドを示すものかを調べる(508)。アプレット登録解除コマンドならばステップ512に移る。さもなくば、それが管理テーブルロックコマンドを示すものかを調べる(509)。管理テーブルロックコマンドならばステップ513に移る。さもなくば、それが管理テーブルアンロックコマンドを示すものかを調べる(510)。管理テーブルアンロックコマンドならばステップ514に移る。さもなくば、ステップ525に移る。

【0068】

ステップ511では、ロックフラグ134を見て、管理テーブル136がアンロック状態かを調べる。ロック状態ならばステップ525に移る。アンロック状態ならば、DataIn606内のAIDと同一のものが既に登録されているAID137の中に存在するか調べる(515)。存在していればステップ525に移る。存在しなければ、管理テーブル136上に空きがあるか(つまり、まだ割り当てられていないセキュアデータブロックが存在するか)を調べる(516)

）。空きがなければステップ525に移る。空があれば、そのセキュアデータブロックに対応するAID137と転送コマンドコード138に、DataIn606に含まれるAIDと転送コマンドコードを設定する(517)。これにより、AIDで示されたアプレットがそのセキュアデータブロックの利用権を獲得する。そして、ステップ526に移る。

【0069】

ステップ512では、ロックフラグ134を見て、管理テーブル136がアンロック状態かを調べる。ロック状態ならばステップ525に移る。アンロック状態ならば、DataIn606内のAIDで、登録されている全てのAID137の中を検索する(518)。一致するAIDを検出したならば(519)、管理テーブル136上からそのAID137とそれに対応する転送コマンドコード138を削除する(520)。一致するAIDを検出しなければステップ525に移る。これにより、AIDで示されたアプレットがそのセキュアデータブロックの利用権を失う。そして、ステップ526に移る。

ステップ513では、ロックフラグ134を見て、管理テーブル136がアンロック状態かを調べる。ロック状態ならばステップ525に移る。アンロック状態ならば、ロックフラグ134にFFhを設定し(521)、管理テーブル136をロック状態にする。DataIn606内のパスワードをパスワードエリア135に設定する(522)。そして、ステップ526に移る。

【0070】

ステップ514では、ロックフラグ134を見て、管理テーブル136がアンロック状態かを調べる。アンロック状態ならばステップ525に移る。ロック状態ならば、DataIn606内のパスワードがパスワードエリア135に設定したものと一致するかを調べる(523)。一致しないならば、ステップ525に移る。一致するならば、ロックフラグ134に00hを設定し(524)、管理テーブル136をアンロック状態にする。そして、ステップ526に移る。

【0071】

ステップ525では、管理コマンドの処理でエラーが発生したことをホスト機器160に示すため、エラー内容を示すステータスコードを含むレスポンスAP

D U 6 1 2 を作り、ステップ 5 2 7 に移る。ステップ 5 2 6 では、管理コマンドの処理が正常に終了したことをホスト機器 1 6 0 に示すため、正常終了（例えば、9 0 0 0 h）というステータスコードを含むレスポンス A P D U 6 1 2 を作り、ステップ 5 2 7 に移る。

【0072】

ステップ 5 2 7 では、レスポンス A P D U 6 1 2 からセキュアリードデータ 6 1 1 を作成する。この後、ホスト機器 1 6 0 はセキュアリードコマンドを発行し（5 2 8）、コントローラチップ 1 2 0 はセキュアリードデータ 6 1 1 を出力する（5 2 9）。そして、ホスト機器 1 6 0 はセキュアリードデータ 6 1 1 を受信する（5 3 0）。

【0073】

尚、本発明の適用に際しては、I C カードチップ 1 5 0 がコントローラチップ 1 2 0 にセキュアデータエリア 1 3 3 へのアクセスを要求する手段として、S W 1 バイト 3 0 5 と S W 2 バイト 3 0 6 に 9 0 F F h という専用のステータス値を設定することを示したが、あくまでこれは一例であり、これ以外の手段でアクセスを要求してもよい。例えば、9 0 F F h 以外のステータスコードでもよいし、D a t a O u t 3 0 4 内に専用のパスワード等を含ませてもよい。

【0074】

尚、本発明の適用に際しては、M M C 1 1 0 が、新たな（あるいは前記の）管理コマンドに応じて、セキュアデータエリア 1 3 3 のサイズを変化させることができる機能を有してもよい。また、新たな（あるいは前記の）管理コマンドに応じて、セキュアデータブロックの分割数（上述では分割数＝4）を変化させることができる機能を有してもよい。また、新たな（あるいは前記の）管理コマンドに応じて、各セキュアデータブロックのサイズを個別に変化させることができる機能を有してもよい。

【0075】

尚、本発明の適用に際しては、上述のパスワードの長さは 2 5 5 バイトでなくともよい。ただし、安全上、このパスワードは長いほうが好ましい。

【0076】

尚、本発明の適用に際しては、アプレット登録解除コマンドで開放されたセキュアデータブロックに、それまでこのブロックを利用していたアプレットに関する機密データが残留し、次にそのブロックの使用権を得た他のアプレットがその機密データを取得する危険性がある。そこで、安全上、登録解除後に残留したデータを消去することが好ましい。その消去の実施は、上述のアプレット登録解除コマンドの処理中におこなってもよいし、MMC 1 1 0 がホスト機器 1 6 0 からの新たな管理コマンドに応じておこなってもよい。

【0 0 7 7】

尚、本発明は、カード形式以外の記憶装置にも適用可能である。

【0 0 7 8】

【発明の効果】

本発明によれば、特定のアプリケーションプログラムに係る処理を実行する場合に、特定のアプリケーションプログラムに係るデータをメモリ装置内部で処理することにより、特定のアプリケーションプログラムに係る処理の安全性を向上できるという効果を奏する。

【0 0 7 9】

本発明によれば、メモリ装置が実行すべきアプリケーションプログラムごとにメモリ装置内のメモリの異なるブロックを割り当てることにより、アプリケーションプログラム間のデータ干渉、即ち、あるアプリケーションプログラムに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制できるという効果を奏する。

【図面の簡単な説明】

【図 1】 本発明を適用したMMCの内部構成を示す図である。

【図 2】 本発明を適用したMMCの動作を概念的に示すフローチャートである。

【図 3】 コントローラチップとICカードチップとの間のICカードコマンドおよびICカードレスポンスの構造を示す図である。

【図 4】 ICカードチップからの要求に応じてフラッシュメモリチップ上のセキュアデータエリアに対するデータの読み書きを実行するフローチャートである。

【図 5】 ICカードチップからの要求に応じてフラッシュメモリチップ上の管理

エリアに対するアプレットの登録およびその解除、また登録情報のロックおよびアンロックを実行するフローチャートである。

【図 6】セキュアライトデータとセキュアリードデータの構成図である。

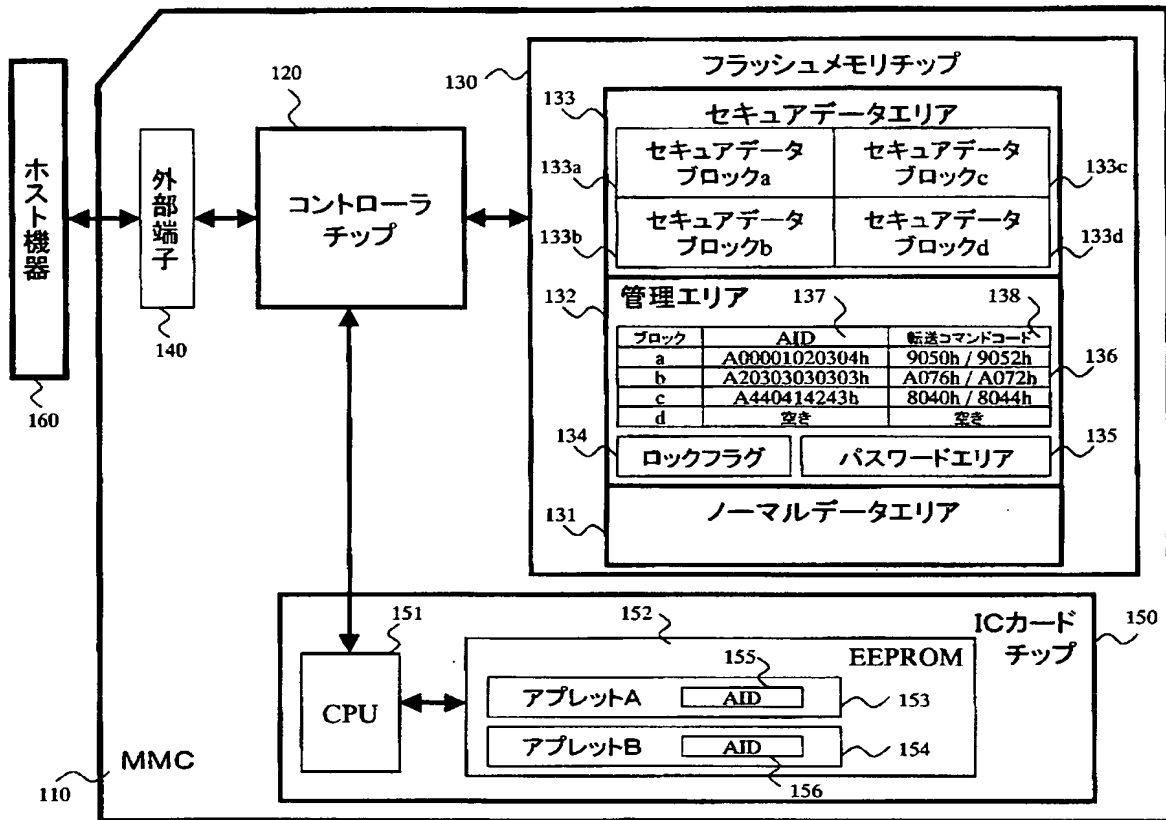
【符号の説明】

1 1 0…MMC、1 2 0…コントローラチップ、1 3 6…管理テーブル、1 4 0…MMC外部端子、1 5 0…ICカードチップ、1 6 0…ホスト機器。

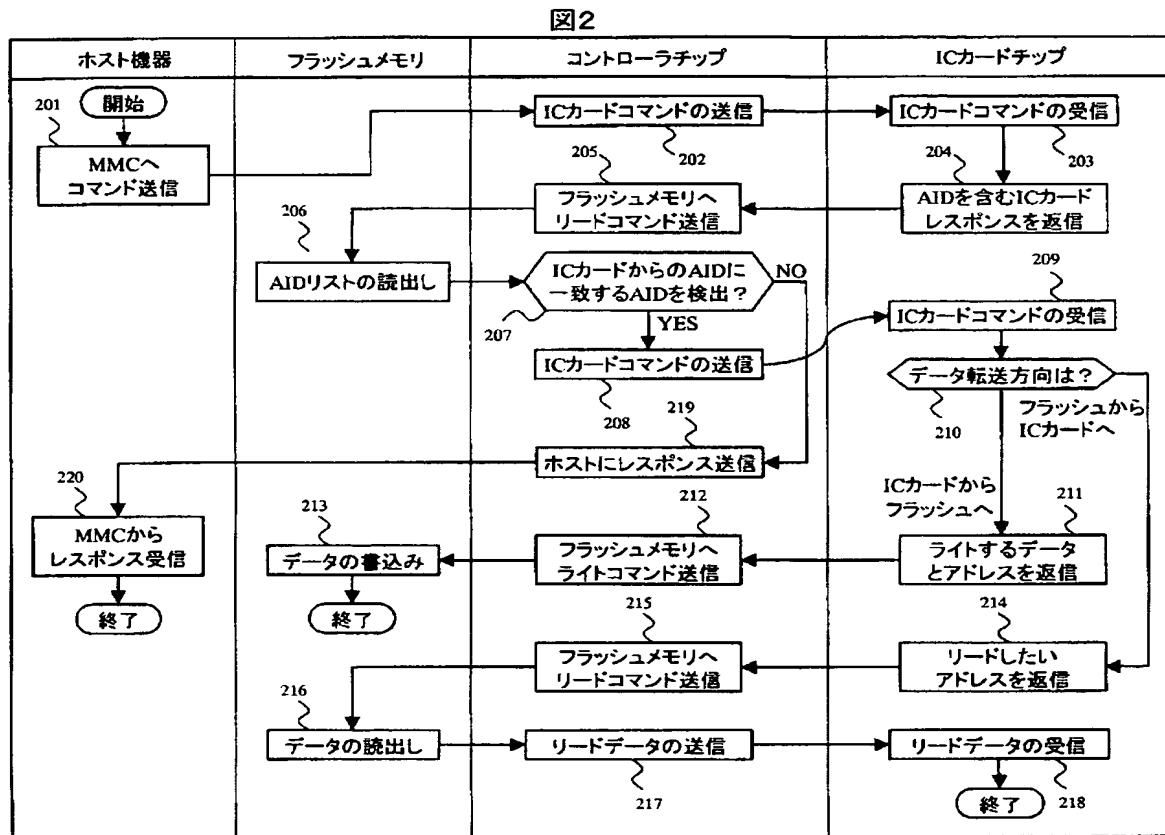
【書類名】 図面

【図 1】

図 1

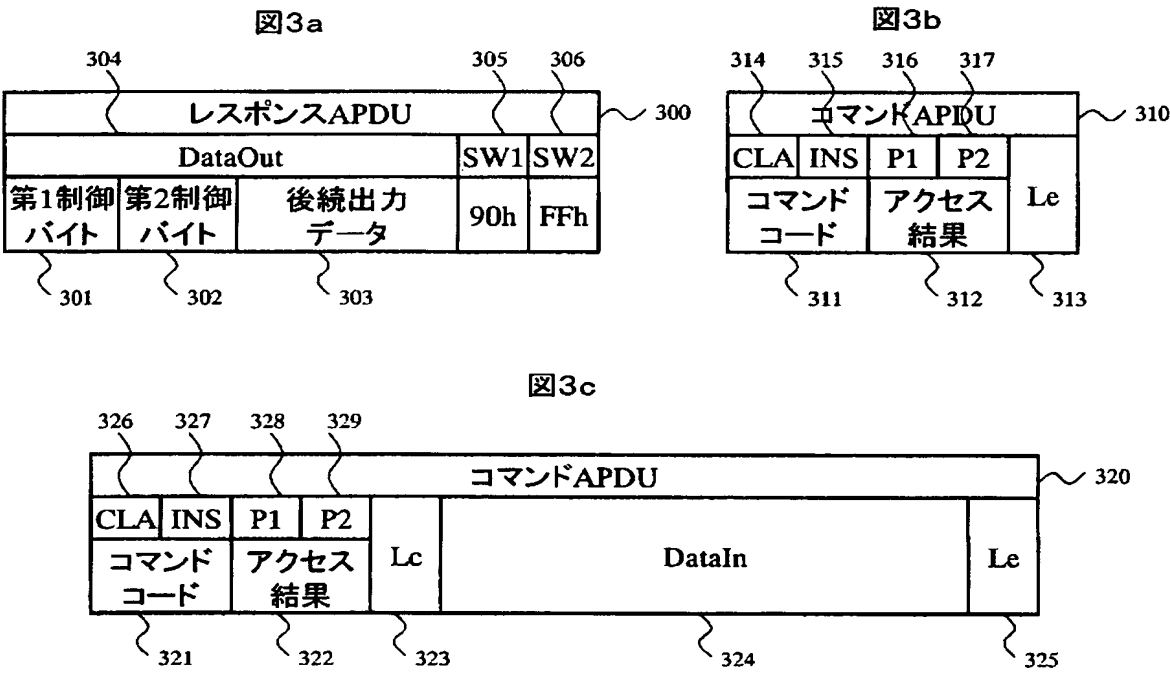


【図2】

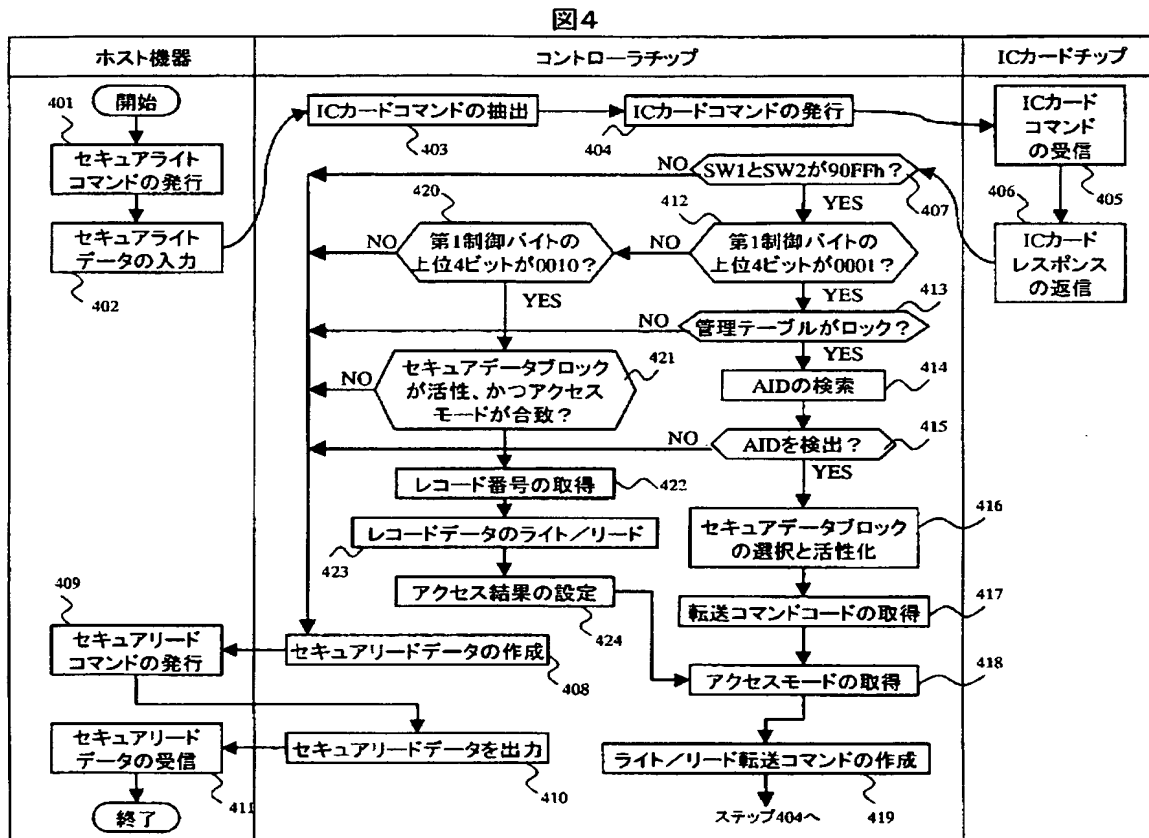


【図 3】

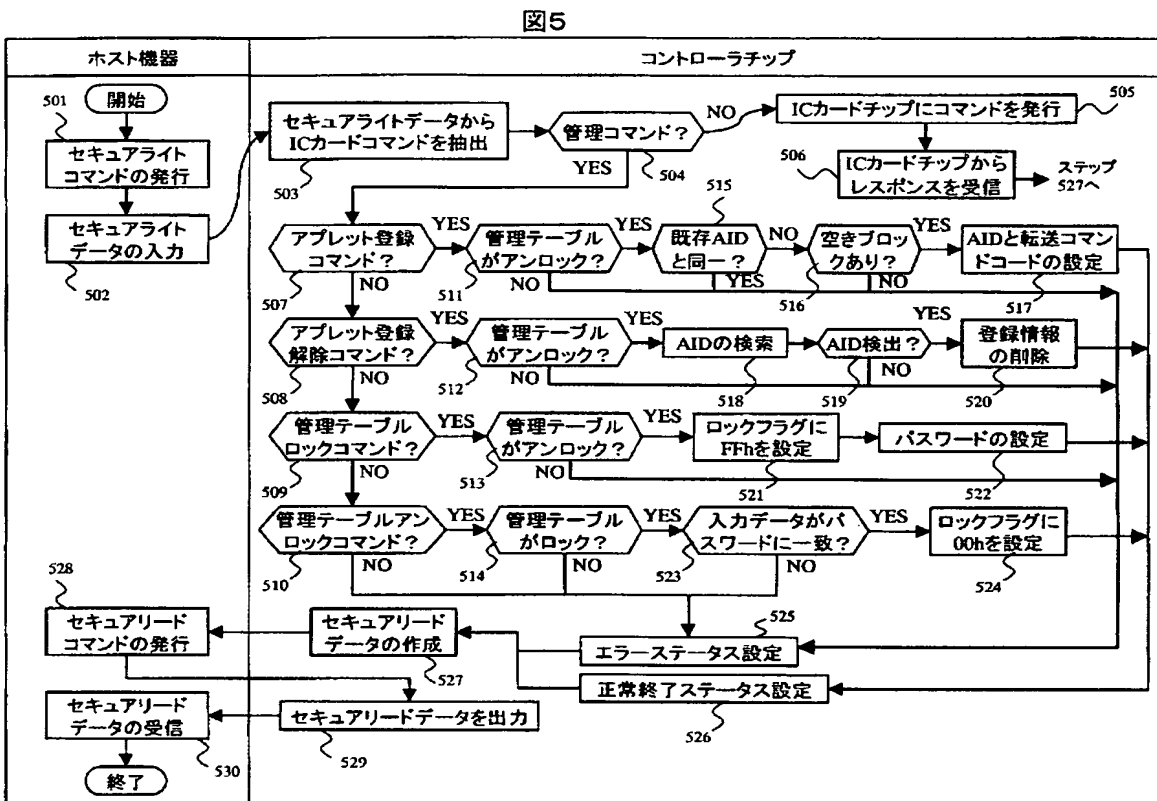
図 3



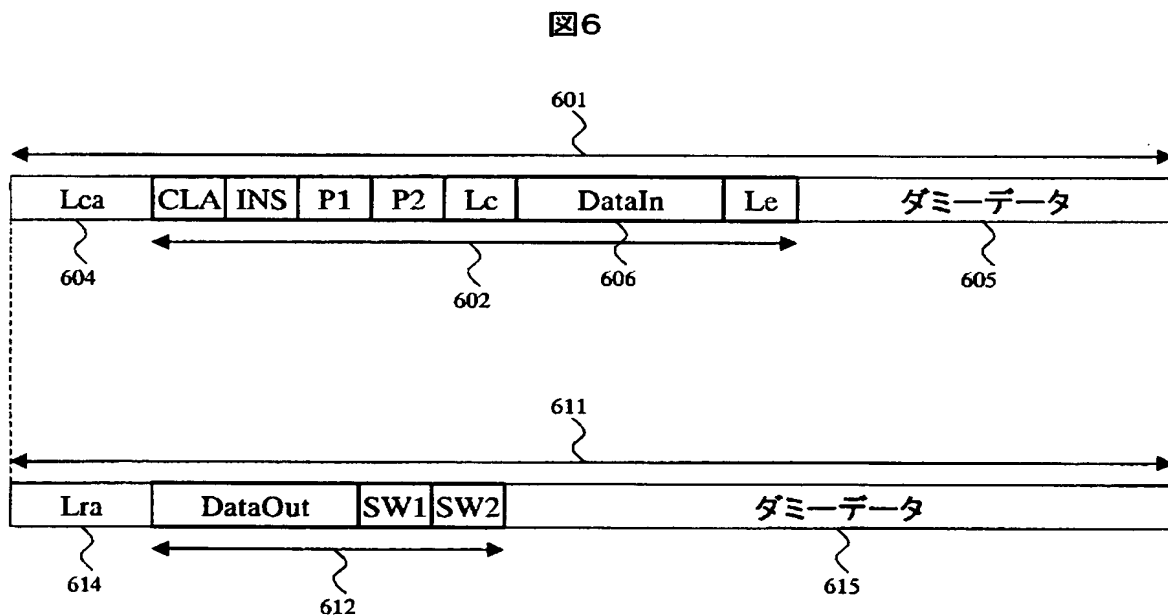
【図4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】

ICカードチップのアプレット間のデータ干渉、即ち、一のアプレットに割り当てられたメモリが他のアプレットにもアクセスされてデータが侵害されることを抑制する。

【解決手段】

本発明は、フラッシュメモリチップ130と、ICカードチップ150と、ホストからの要求に応じてフラッシュメモリチップ及びICカードチップへのデータの読み書きを制御するコントローラチップ120とを備え、フラッシュメモリチップは、ホスト機器からのデータを記憶するためのノーマルデータエリア131とICカードチップからのデータを記憶するためのセキュアデータエリア133を有し、さらに、セキュアデータエリア133は、アプレット153, 154ごとに割り当てられたセキュアデータブロック133a, 133b, 133c, 133dに分割される。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 5 0 2 4 3
受付番号	5 0 3 0 0 3 1 3 9 3 1
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 3 月 4 日

< 認定情報・付加情報 >

【提出日】	平成15年 2月27日
-------	-------------

次頁無

【書類名】 出願人名義変更届（一般承継）

【あて先】 特許庁長官 殿

【事件の表示】

【出願番号】 特願2003- 50243

【承継人】

【識別番号】 503121103

【氏名又は名称】 株式会社ルネサステクノロジ

【承継人代理人】

【識別番号】 100080001

【弁理士】

【氏名又は名称】 筒井 大和

【提出物件の目録】

【包括委任状番号】 0308729

【物件名】 承継人であることを証明する登記簿謄本 1

【援用の表示】 特許第 3 1 5 4 5 4 2 号 平成 1 5 年 4 月 1 1 日付け
提出の会社分割による特許権移転登録申請書 を援用
する

【物件名】 権利の承継を証明する承継証明書 1

【援用の表示】 特願平 1 - 2 5 1 8 8 9 号 同日提出の出願人
名義変更届（一般承継）を援用する

【プルーフの要否】 要

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 5 0 2 4 3
受付番号	5 0 3 0 1 4 0 3 5 3 5
書類名	出願人名義変更届（一般承継）
担当官	土井 恵子 4 2 6 4
作成日	平成 1 5 年 1 1 月 4 日

<認定情報・付加情報>

【提出日】 平成15年 8月26日

特願 2 0 0 3 - 0 5 0 2 4 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所

特願 2 0 0 3 - 0 5 0 2 , 4 3

出 願 人 履 歴 情 報

識別番号

[5 0 3 1 2 1 1 0 3]

1. 変更年月日

2 0 0 3 年 4 月 1 日

[変更理由]

新規登録

住 所

東京都千代田区丸の内二丁目 4 番 1 号

氏 名

株式会社ルネサステクノロジ